Appendix 1

Privacy impact assessment on use of CCTV at Council Owned Community Managed Community Centres.

Creggan Neighbourhood Partnership, Mullabouy Community Centre, Shantallow Community Centre and Tullyally Community Centre.

External and Internal CCTV cameras were fitted to four Community Centres at a time of renovation and capital expenditure. These cameras cover all external areas around the buildings. These cameras cover internal corridors and entrance hallways of the buildings.

Background

Close Circuit Television (CCTV) is visual surveillance technology designed to monitor a variety of environments and activity. The Data Protection Act 1998 regulates the processing of personal and sensitive personal data. The Act impacts upon the use of CCTV if images that focus on an individual are recorded.

CCTV can be used to combat a variety of offending activity; in this instance, the focus will be on the security of the building, deterrent of thefts and possible assaults to council staff.

The Information Commissioner's Office (ICO) has issued a Code of Practice (COP) relating to CCTV and this provides standards the ICO considers good practice on the processing of images and footage. It sets out how a Data Controller should manage the overall processing of CCTV data. This is a very important part of meeting compliance with the Act and the COP has been considered in the development of this document.

The personal data processed as part of the CCTV system is controlled by Derry City & Strabane District Council who is the Data Controller of the personal data recorded for this purpose by all cameras on this system.

Information flows

The use of CCTV cameras will fall into the category of **"overt recording"** and is not subject to the Regulation of Investigatory Powers Act 2000 (RIPA). They are not to be used in a hidden or covert manner.

CCTV will capture individuals both externally in the external walls of the Community Centre's boundaries and internal public entrances.

Location: There are currently four Community Centres covered by CCTV cameras covering the external of the building including car parks and CCTV cameras inside the Centres covering corridors and reception areas and halls.

Details:

All internal cameras are in a fixed position, all external cameras are fixed.

- The cameras will have sight of individuals and vehicles approaching the areas from a distance.

- The cameras will observe staff and members of the public using the facility.

- Cameras may also capture images of public roadways & walkways but the Code of Practice will ensure that surveillance will not be used to survey the interior of private premises or to harass or intimidate any individual or group.

CCTV Public Surveillance Camera Controlled by DCSDC

Location: Creggan Neighbourhood Partnership, Central Drive, Creggan, Derry, BT489QG

Number of Cameras	13
Age of	Internal: 3 years, External: 3 Years

System	
Temporary or Permanent	Permanent
Type of Camera	Monitored 24/7/365
Record or Download	Record
Overwrite Time	31 days

Location of Control Unit: Creggan Neighbourhood Partnership, Central Drive, Creggan, BT489QG

Who Has Access: Trained operators with responsibility for using the equipment housed within Council Offices, 98 Strand Rd, Derry, BT487NN

CCTV Public Surveillance Camera Controlled by DCSDC

Location: Mullabouy Community Centre, Lettershandoney Avenue, Lettershandoney, BT473HY.

Number of Cameras	12
Age of Cameras	Internal 2 years External 2 years
System	
Temporary or Permanent	Permanent
Record or Download	Record

Overwrite Period	31 days.

Location of Control Unit: Mullabouy Community Centre, Lettershandoney Ave, Lettershandoney, BT473HY

Who Has Access: Trained operators with responsibility for using the equipment housed within Council Offices, 98 Strand Rd, Derry, BT487NN.

CCTV Public Surveillance Camera Controlled by DCSDC

Location: Shantallow Community Centre, 38 Drumleck Drive, Shantallow, Derry, BT488EN.

Number of Cameras	13
Age of Cameras	Internal 5 years External 5 years
System	
Temporary or Permanent	Permanent
Record or Download	Record

Overwrite Period	31 days.

Location of Control Unit: Shantallow Community Centre, 38 Drumleck Drive, Derry, BT488EN

Who Has Access: Trained operators with responsibility for using the equipment housed within Council Offices, 98 Strand Rd, Derry, BT487NN.

CCTV Public Surveillance Camera Controlled by DCSDC

Location: Tullyally Community Centre, Glendermott Business Park, Tullyally Rd, Derry, BT473QR.

Number of Cameras	12
Age of Cameras	Internal 3 years External 3 years
System	
Temporary or Permanent	Permanent
Record or Download	Record
Overwrite Period	31 days.

Location of Control Unit: Tullyally Community Centre, Glendermott Business Park, Tullyally Rd, Derry, BT473QR.

Who Has Access: Trained operators with responsibility for using the equipment housed within Council Offices, 98 Strand Rd, Derry, BT487NN.

Control Processes for Derry City and Strabane District Council CCTV Cameras

Service Area	Health and Community, Community and Leisure, Community Development.
Location	Council Offices, 98 Strand Road, Derry BT48 7NN

Purpose for which CCTV is processed	Prevent crime, prevent, deter and detect crime, apprehend and prosecute offenders, administration of Community Centres.
When was this purpose reviewed and is its use proportionate to the issue/problem	Reviewed 2014 and deemed proportionate to problem

Who has access to the Council Owned and Community Managed Community Centre CCTV footage: Trained operators with responsibility for using the equipment housed within the CCTV Control Centre

Is this access to live or recorded footage or both	Both	
Who responsible for the control of the of the information (data controller)		Facilities Coordinator and Community Services Manager
Who is resp. for deciding what is recorded	All recorded	
Who is resp. for deciding where the CCTV is set up		
Who is resp. for deciding how the info is used	Data Controller,	Facilities Coordinator and Community Services Manager
Who authorises the release of CCTV footage	Data Controller,	Facilities Coordinator and Community Services Manager
Who is resp for storage of the information	DCSDC	
Who is resp for deletion of the information	DCSDC	

Consultation requirements

The use of CCTV has been discussed at a full council meeting on 23/04/2013 and approved as a tool to create a safe and secure environment for all those who visit, work and do business in the Derry City and Strabane District Council offices. CCTV is a method of reducing fear of crime/reassuring the public, helping prevent crime, deterring and detecting crime, helping to identify, apprehend and prosecute offenders, providing evidence for criminal and civil action in the courts.

What is the organisation's purpose for using CCTV? What are the problems it is meant to address?

To enhance the safety and well-being of staff and the public (particularly children and adults at risk of harm) using Council premises and services;
- To prevent, investigate and detect crime and to assist with the apprehension and prosecution of offenders;
- To discourage anti-social behaviour including dog fouling and littering;
- To assist with insurance claims, investigations and the overall management and supervision of Council buildings, premises and events;
- To facilitate disciplinary investigations where criminal activity or breaches of health, safety and wellbeing of staff and facility users may have taken place

What are the views of those who will be under surveillance?

The general feeling is that staff who are not involved in crime are happy to be in an area that is monitored by CCTV cameras. There are some members of staff both law abiding and those who are not, who have issues with being in areas covered by CCTV cameras. By adhering to current legislation the CCTV system is only used for agreed purposes and but it may also discourage other forms of unacceptable behaviour and crime.

What are the benefits to be gained from its use?

Staff, visitors and businesses will benefit from improved detection of thefts & threats and associated crime.

CCTV is a proven tool in detecting offences, and the perpetrators of it. Using CCTV will significantly reduce the time and cost on the PSNI in investigating allegations.

CCTV captures actual events and is not influenced by interpretation. CCTV also helps prevent offences.

The deployment of CCTV camera technology will produce a number of benefits for staff including:

- Reducing the fear of crime and reassuring the public.
- Helping prevent crime
- Deterring and detecting crime
- Helping to identify, apprehend and prosecute offenders
- Providing evidence for criminal and civil action in the courts

What could you do to minimize intrusion for those that may be monitored, particularly if specific concerns have been expressed?

Public surveillance CCTV located in the Derry City and Strabane District Council Community Centres are governed by a Code of Practice (June 2017, Doc No: CORP 30/16) which commits to the highest standards of professionalism and integrity with regard to safeguarding individual rights and privacy. The Code of Practice states that CCTV surveillance will not be used to invade the privacy of individuals or to harass and intimidate any individual or group. All of our CCTV cameras will be used on a proper and legal basis, comply with the Data Protection Act and regular reviews of camera performance will be undertaken to justify its need.

Can CCTV technology realistically deliver these benefits?

Yes. The existing cameras have consistently deterred crime, enhanced staff safety since installed. The evidence pertaining to this is that there have been no incidents since cameras were installed.

Do you need images of identifiable individuals, or could the scheme use other images not capable of identifying the individual?

All cameras are capable of identifying individuals, as footage from the system may be used for enforcement and prosecution. The camera requires this capability to ensure it is fit for purpose as identifiable images are required for prosecution purposes for both crimes committed and any health and safety infringements.

Will the particular equipment/system of work being considered deliver the desired benefits now and remain suitable in the future?

Yes, although any camera which is found not fit for purpose will be replaced with one that is.

What future demands may arise for wider use of images and how will you address these?

Legislation may change and we will comply with all future regulations placed upon Council. Any request to use the images captured will be made in writing to the Data Controller and these requests are considered in line with the Council's Data Protection Policy and CCTV policy.

Due to the overt nature of CCTV, the signage displayed and the information provided, individuals will be aware of the location/positioning of CCTV cameras in the Council Offices.

Identify the privacy and related risks

Annex three was used to help identify the DPA related compliance risks.

Privacy issue	Risk to individuals	Compliance risk	Associated organisation / corporate risk
Inadequate disclosure controls	Increase the likelihood of Information/images of the general public being shared inappropriately.	Non-compliance with the DPA. Non-compliance with the Privacy and Electronic Communications Regulations (PECR).	Council reputation and possible litigation Non-compliance with the DPA or other legislation can lead to sanctions, fines, legal challenges and reputational damage.
The information being used for a different purpose	The context in which information is used or disclosed can change over time, leading to it being used for different purposes without	Non-compliance with sector specific legislation or standards. Non-compliance with human	Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, is less useful to the business.

	people's knowledge. Could lead to an unjustified intrusion on people's privacy.	rights legislation.	Public distrust about how information is used can damage an organisation's reputation and lead to loss of business/engagement.
CCTV surveillance methods and measures are unnecessary	The sharing and merging of datasets can allow organisations to collect a much wider set of information than individuals might expect.		Data losses which damage individuals could lead to claims for compensation.
Inappropriate use and sharing of information.	Vulnerable people at risk may be particularly concerned about the risks of identification or the disclosure of information.		Possible prosecution by the ICO. Damage to Councils reputation.
Disclosure of information capturing Vulnerable/At Risk Individuals	Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, presents an increased security risk.		Improper Disclosure of information. Improper use of footage.

Inappropriate storage or duplication of collected information. Collected information being retained for too long.	If a retention period is not established information might be used for longer than necessary		Inappropriate storage of data. In breach of Councils Retention & Disposal policy if information is kept too long.

Identify privacy solutions

Risk	**Solution(s)**	**Result:** is the risk eliminated, reduced, or accepted?	**Evaluation:** is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?
Inadequate disclosure controls	Controls put in place in accordance with Council's CCTV policy and CCTV Code of Practice to ensure that information held on staff and the general public is not shared inappropriately.	Eliminated	Yes

The information being used for a different purpose	Controls put in place in accordance with Council's CCTV policy, DPA, PECR and CCTV Code of Practice to ensure that information on staff and the general public is not shared inappropriately. Legislation may change and we will comply with all future regulations. The demand for wider use of images is regulated by the Data Controller with all requests submitted in writing.	Reduced	Yes

	PSNI must also submit a viewing request to the Data Controller before any access to the images is granted. DCSDC are the Data Controller who decides if images are released to any organisations. As Data Controller for the system, DCSDC has the legal responsibility in relation to images authorised for release.		
CCTV surveillance methods and measures are unnecessary	CCTV will only be used in areas where there is a problem of nuisance and crime when all other methods/interventions have	Eliminated	Yes

	been exhausted, tried or deemed ineffective.		
Inappropriate use and sharing of information	CCTV information will only be shared when authorised by the Data Controller for the purposes preventing and deterring unacceptable behaviour and crime. Images are recorded 24/7/365 and will only be released to other law enforcement agencies such	Eliminated	Yes

	as the PSNI if the Data Controller deems that a legitimate request has been received. DCSDC will be the Data Controller at the point of images being recorded, however if any images are released to any of the authorised organisations, then the legal responsibility will be transferred to that organisation in relation to the images that have been released.		

Disclosure of information capturing Vulnerable people	Controls put in place in accordance with Council's CCTV policy, DPA, PECR and CCTV Code of Practice to ensure that information relating to vulnerable people is not shared inappropriately.	Eliminated	Yes
Inappropriate storage or duplication of collected information.	Controls put in place in accordance with Council's CCTV policy, DPA, PECR and CCTV Code of Practice to ensure that all images are stored appropriately. Those monitoring the images are also fully accredited.	Eliminated	Yes
		Eliminated	Yes

Collected information being retained for too long.	Images stored on HD-CCTV DVR HD1600F-R (SCC) HD-CCTV EH1600L (CNP,TCC,MCC) All CCTV images are recorded and held for 31 days. Relevant information/images held pending investigation and prosecution are retained for periods recommended under the Code of Practice.		

Sign off and record the PIA outcomes

Who has approved the privacy risks involved in the project? What solutions need to be implemented?

Risks	Approved solutions	Approved by
Inadequate disclosure controls	Controls put in place in accordance with Council's CCTV policy, DPA, PECR and CCTV Code of Practice to ensure that: Information of general public, vulnerable people is not shared inappropriately. Information is not collected and stored unnecessarily.	Barry O'Hagan Head of Service
The information being used for a different purpose	Information is properly managed to avoid the creation of duplicate records.	
CCTV surveillance methods and measures are unnecessary Inappropriate use and sharing of information	Information/images are deleted after 31 days, relevant information is held pending investigation and prosecution	
Disclosure of information capturing Vulnerable people	Controls put in place in accordance with Council's CCTV policy, DPA, PECR and CCTV	

Inappropriate storage or duplication of collected information. Collected information being retained for too long.	Code of Practice to ensure that: Information of general public, vulnerable people is not shared inappropriately. Information is not collected and stored unnecessarily. Information is properly managed to avoid the creation of duplicate records. Images will only be held for 31 days	

Integrate the PIA outcomes back into the project plan

Action to be taken	Date for completion of actions	Responsibility for action
Integrate the PIA outcomes back into the CCTV policy/plan.	31st March 2018	Susan Mullan

Contact point for future privacy concerns
Susan Mullan

Annex three

Linking the PIA to the data protection principles

Answering these questions during the PIA process will help you to identify where there is a risk that the project will fail to comply with the DPA or other relevant legislation, for example the Human Rights Act.

Principle 1

Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:

a) at least one of the conditions in Schedule 2 is met, and

b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

Have you identified the purpose of the project?

How will you tell individuals about the use of their personal data?

Do you need to amend your privacy notices?

Have you established which conditions for processing apply?

If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?

If your organisation is subject to the Human Rights Act, you also need to consider:

Will your actions interfere with the right to privacy under Article 8?

Have you identified the social need and aims of the project?

Are your actions a proportionate response to the social need?

Principle 2

Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

Does your project plan cover all of the purposes for processing personal data?

Have you identified potential new purposes as the scope of the project expands?

Principle 3

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

Is the quality of the information good enough for the purposes it is used?

Which personal data could you not use, without compromising the needs of the project?

Principle 4

Personal data shall be accurate and, where necessary, kept up to date.

If you are procuring new software does it allow you to amend data when necessary?

How are you ensuring that personal data obtained from individuals or other organisations is accurate?

Principle 5

Personal data processed for any purpose or purposes shall not be kept for longer than necessary for that purpose or those purposes.

What retention periods are suitable for the personal data you will be processing?

Are you procuring software that will allow you to delete information in line with your retention periods?

Principle 6

Personal data shall be processed in accordance with the rights of data subjects under this Act.

Will the systems you are putting in place allow you to respond to subject access requests more easily?

If the project involves marketing, have you got a procedure for individuals to opt out of their information being used for that purpose?

Principle 7

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Do any new systems provide protection against the security risks you have identified?

What training and instructions are necessary to ensure that staff know how to operate a new system securely?

Principle 8

Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country of territory ensures and adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Will the project require you to transfer data outside of the EEA?

If you will be making transfers, how will you ensure that the data is adequately protected?